PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : G06F 11/20, 12/14

A1

(11) Numéro de publication internationale: WO 00/36511

(43) Date de publication internationale: 22 juin 2000 (22.06.00)

(21) Numéro de la demande internationale: PCT/FR99/03086

(22) Date de dépôt international: 10 décembre 1999 (10.12.99)

(30) Données relatives à la priorité:
98/15650 11 décembre 1998 (11.12.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: BULL CP8 [FR/FR]; 68, route de Versailles, Boîte postale 45, F–78430 Louveciennes (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: DIENER, Sébastien [FR/FR]; 50 boulevard Foch, F–22410 Saint Quay Portrieux (FR). TRIERWEILER, Franz [FR/FR]; 57, rue Exelmans, F–78000 Versailles (FR).

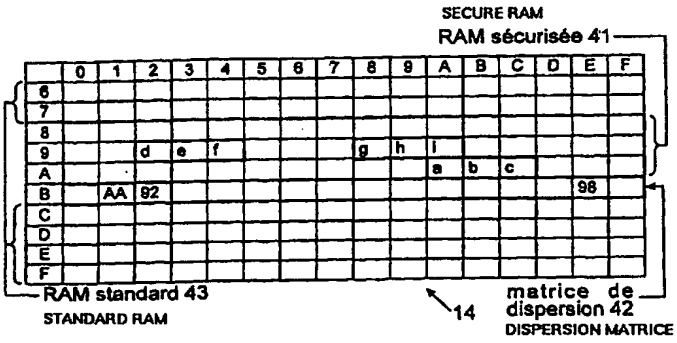
(74) Mandataire: CORLU, Bernard; Bull S.A., PC58D20, 68, route de Versailles, F–78434 Louveciennes Cedex (FR).

(81) Etats désignés: US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD FOR STORING AND OPERATING DATA UNITS IN A SECURITY MODULE AND ASSOCIATED SECURITY MODULE

(54) Titre: PROCEDE DE STOCKAGE ET D'EXPLOITATION D'UNITES D'INFORMATION DANS UN MODULE DE SECURITE, ET MODULE DE SECURITE ASSOCIE



(57) Abstract

The invention concerns a method for storing data in data storage means of a security module. The invention is characterised in that it consists in defining two storage zones (41, 42) whereof one (41) is designed to store data (a, b, c; d, e, f) by dispersed sections (a, b, c) (d, e, f) and the other (42) is designed to store addresses (AA, 92) where the data sections are located. The storage in the second storage zone is carried out in positions which are based on the address (83, 86) of the data sections in the first storage zone (41), as defined before dispersion. The invention also concerns a method for operating data units in a security module, and the associated security module.

(57) Abrégé

L'invention concerne un procédé de stockage d'informations dans des moyens de stockage d'information d'un module de sécurité. Selon l'invention, on définit deux zones mémoire (41, 42), dont une (41) est destinée à stocker les informations (a,b,c; d,e,f) par morceaux dispersés (a,b,c), (d,e,f), et l'autre (42) est destinée à stocker des adresses (AA,92) où se trouvent les morceaux d'informations. Le stockage dans la seconde zone mémoire s'effectue en des positions qui sont fonction de l'adresse (83,86) des morceaux d'informations dans la première zone mémoire 41, telle que définie avant dispersion. L'invention concerne aussi un procédé d'exploitation d'unités d'information dans un module de sécurité, et le module de sécurité associé.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

Procédé de stockage et d'exploitation d'unités d'information dans un module de sécurité, et module de sécurité associé

L'invention concerne un procédé de stockage et d'exploitation d'unités d'information dans un module de sécurité. Le terme "module de sécurité" doit être pris, soit dans son sens classique dans lequel il désigne un dispositif ayant vocation, dans un réseau de communication ou d'information, à être détenu par un organisme supervisant le réseau et à stocker de façon protégée des paramètres secrets et fondamentaux du réseau tels que des clés cryptographiques, soit comme désignant plus simplement un dispositif attribué à divers usagers du réseau et permettant à chacun d'eux d'avoir accès à celui-ci, ce dernier dispositif étant lui aussi susceptible de détenir des paramètres secrets. Le module de sécurité pourra prendre la forme d'un objet portatif du type carte à puce.

On sait qu'un fraudeur est susceptible de lire ou d'altérer des informations contenues dans des moyens de stockage d'information, notamment dans des mémoires de puces électroniques, en utilisant selon les cas un microscope électronique ou des moyens de production de rayonnements. Toutefois, pour être efficace, il lui faut non seulement accéder aux informations stockées, mais aussi identifier la fonction de ces informations dans le fonctionnement du module de sécurité.

Le but principal de l'invention est de proposer un procédé de stockage d'informations permettant de rendre beaucoup plus difficile le repérage de la fonction attribuée à chacune des informations stockées.

L'invention concerne à cet effet un procédé de stockage d'informations dans des moyens de stockage d'information d'un module de sécurité, caractérisé en ce qu'il comprend les étapes consistant à :

-définir, dans les moyens de stockage, une première zone mémoire destinée à stocker des informations, accessibles en désignant des adresses logiques ;

-définir, dans les moyens de stockage, une seconde zone mémoire destinée à stocker des adresses physiques de ces informations définissant leur position dans la première zone mémoire, ces adresses physiques étant situées en une position qui est fonction des adresses logiques respectives des informations ;

-stocker les informations dans la première zone mémoire en une position qui est fonction de leurs adresses logiques respectives, et les adresses logiques de ces informations dans la seconde zone mémoire en une position qui est fonction de ces adresses logiques ; et

-permuter deux à deux les adresses logiques des unités d'information dans la seconde zone mémoire pour définir leurs adresses physiques et, après chaque permutation, permuter les deux unités d'information correspondantes dans la première zone mémoire, ou vice versa.

En variante, le procédé de stockage d'informations dans des moyens de stockage d'information d'un module de sécurité, est caractérisé en ce qu'il comprend les étapes consistant à :

-définir, dans les moyens de stockage, une première zone mémoire destinée à stocker des informations, accessibles en désignant des adresses logiques ;

-définir, dans les moyens de stockage, une seconde zone mémoire destinée à stocker des adresses physiques de ces informations définissant leur position dans la première zone mémoire, ces adresses physiques étant situées en une position qui est fonction des adresses logiques respectives des informations ;

-stocker aléatoirement dans la seconde zone mémoire les adresses logiques des informations pour définir des adresses physiques de ces informations ; et

-stocker les informations dans la première zone mémoire en une position qui est fonction de leurs adresses physiques respectives.

Ainsi, les informations se trouvent être dispersées dans les moyens de stockage, ce qui empêche en pratique leur repérage. Des perfectionnements, exposés dans le présent document, permettent en outre de protéger encore davantage les informations stockées.

L'invention concerne aussi un procédé d'exploitation et un module de sécurité correspondants.

D'autres détails et avantages de la présente invention apparaîtront au cours de la description suivante, d'un mode d'exécution préféré mais non limitatif, en regard des dessins annexés sur lesquels :

La figure 1 représente un dispositif de traitement de données coopérant avec un module de sécurité ;

La figure 2 représente une variante de module de sécurité ;

La figure 3 représente une mémoire volatile d'un module de sécurité , incorporant deux zones mémoire particulières, constituant respectivement une mémoire RAM sécurisée et une matrice de dispersion ;

La figure 4 représente la mémoire de la figure 3, après dispersion des unités d'information de la mémoire RAM sécurisée 41 ;

La figure 5 est une variante de la figure 4, où les unités d'information occupent chacune une seule cellule de mémoire ;

La figure 6 illustre le repérage des cellules à partir d'un pointeur ;

La figure 7 est un organigramme d'une procédure d'inversion de deux cellules de la matrice de dispersion ;

Les figures 8 à 10 représentent la mémoire volatile, lors de trois étapes successives de la procédure de la figure 7 ;

La figure 11 est un organigramme d'une procédure d'inversion de deux cellules de la mémoire RAM sécurisée, faisant suite à la procédure de la figure 7 ;

Les figures 12 à 14 représentent la mémoire volatile, lors de trois étapes successives de la procédure de la figure 11 ; et

La figure 15 est un organigramme d'une procédure de permutation multiple des cellules de la mémoire RAM sécurisée.

La figure 1 représente un dispositif de traitement de données 1 coopérant avec un objet portatif 8. Le dispositif de traitement de données comprend de façon connue en soi un microprocesseur 2 auquel sont reliés une mémoire ROM 3, et une mémoire RAM 4, des moyens 5 pour coopérer, avec ou sans contact physique, avec l'objet portatif 8, et une interface de transmission 7 permettant au dispositif de traitement de données de communiquer avec un réseau de communication de données. Le dispositif de traitement de données 1 peut en outre être équipé de moyens de stockage tels que des disquettes ou disques amovibles ou non, de moyens de saisie (tels qu'un clavier et/ou un dispositif de pointage du type souris) et de moyens d'affichage, ces différents moyens n'étant pas représentés sur la figure 1.

Le dispositif de traitement de données peut être constitué par tout appareil informatique installé sur un site privé ou public et apte à fournir des moyens de gestion de l'information ou de délivrance de divers biens ou services, cet appareil étant installé à demeure ou portable. Il peut notamment s'agir aussi d'un appareil dédié aux télécommunications.

Par ailleurs, l'objet portatif 8 porte une puce incluant des moyens de traitement de l'information 9, une mémoire non volatile 10, une mémoire volatile de travail RAM 14, et des moyens 13 pour coopérer avec le dispositif de traitement de données 1. Cette puce est agencée pour définir, dans la mémoire 10, une zone secrète 11 dans laquelle des informations une fois enregistrées, sont inaccessibles depuis l'extérieur de la puce mais seulement accessibles aux moyens de traitement 9, et une zone accessible 12 qui est rendue accessible depuis l'extérieur de la puce par le microprocesseur 9 pour une lecture et/ou une écriture d'informations. Chaque zone de la mémoire non

volatile 10 peut comprendre une partie non modifiable ROM et une partie modifiable EPROM, EEPROM, ou constituée de mémoire RAM du type "flash" ou FRAM (cette dernière étant une mémoire RAM ferromagnétique), c'est-à-dire présentant les caractéristiques d'une mémoire EEPROM avec en outre des temps d'accès identiques à ceux d'une RAM classique.

En tant que puce, on pourra notamment utiliser un microprocesseur autoprogrammable à mémoire non volatile, tel que décrit dans le brevet américain n° 4.382.279 au nom de la Demanderesse. Comme indiqué en colonne 1, lignes 13-25 de ce brevet, le caractère autoprogrammable de la puce correspond à la possibilité pour un programme fi situé dans une mémoire ROM, de modifier un autre programme fj situé dans une mémoire programmable en un programme gj. Dans une variante, le microprocesseur de la puce est remplacé - ou tout du moins complété - par des circuits logiques implantés dans une puce à semi-conducteurs. En effet, de tels circuits sont aptes à effectuer des calculs, notamment d'authentification et de signature, grâce à de l'électronique câblée, et non microprogrammée. Ils peuvent notamment être de type ASIC (de l'anglais « Application Specific Integrated Circuit »).

Une variante de la figure 1 est illustrée sur la figure 2, où le dispositif de traitement de données 16 comprend, outre les éléments du dispositif de traitement de données 1 de la figure 1, ceux de l'objet portatif 8 disposés dans un module 15, les éléments communs aux deux figures 1,2 portant les mêmes références. Toutefois, les moyens de coopération 5,13 de la figure 1 sont remplacés par une liaison permanente entre le microprocesseur 2 et le microprocesseur 9.

Selon une variante de la figure 2, le dispositif de traitement de données est constitué par le module 15 de la figure 2 lui-même.

Selon l'invention, l'emplacement physique et la structure d'une information sensible dans une des mémoires de l'objet portatif 8 ou du

module 15 évolue dans le temps de façon aléatoire. Soit S un ensemble de n cellules mémoire (c0, c1, c2, ..., c(n-1)) et f une fonction de dispersion propre à disperser le contenu d'une quelconque cellule c_i depuis une adresse originelle jusqu'à une adresse dispersée $f(c_i)$. La fonction f vérifie les deux propriétés suivantes :

$$c_i \neq c_j \Rightarrow f(c_i) \neq f(c_j)$$

$$c_i \in S \Rightarrow f(c_i) \in S$$

(où $\in$ est un symbole signifiant « appartenant à »)

A titre d'exemple, est représentée sur la figure 3 la structure de la mémoire RAM 14 de l'objet portatif 8 ou du module 15. Elle comporte seize colonnes identifiées par les chiffres 0 à 9 puis par les lettres A à F (notation hexadécimale), ainsi que dix lignes identifiées par les chiffres 6 à 9 puis par les lettres A à F. Ces lignes et colonnes définissent cent soixante cellules repérées depuis la cellule 60 (c'est-à-dire ligne 6, colonne 0) jusqu'à la cellule FF (c'est-à-dire ligne F, colonne F). Chaque cellule stocke un octet binaire.

La mémoire RAM est décomposée en trois zones différentes. Une première zone 41 comprend les cellules 80 à AF et est nommée « mémoire RAM sécurisée » car son contenu va être sécurisé au moyen de la fonction f précitée : c'est dans cette zone que vont être stockées des informations sensibles à protéger. Une deuxième zone 42 comprend les cellules B0 à BF et est nommée « matrice de dispersion » car elle va être utilisée pour disperser les informations sensibles dans la mémoire RAM sécurisée. Enfin, une troisième zone 43, dite « mémoire RAM standard », comprend les cellules restantes, à savoir 60 à 7F et C0 à FF : elle est utilisée pour stocker les informations non sensibles. On notera que si, dans cet exemple, la mémoire RAM sécurisée et la matrice de dispersion sont composées de cellules contigües, elles pourraient, en variante, être composées de cellules non contigües.

Selon une forme de réalisation préférée, l'ensemble des informations stockées dans la mémoire RAM sécurisée est décomposé en plusieurs éléments appelés « unités d'information » comprenant chacune un même nombre déterminé de cellules. Dans l'exemple des figures 3 et 4, chaque unité d'information est entourée d'un trait fort et comprend trois cellules : on distingue par exemple l'unité d'information (a,b,c) dont le contenu est réparti dans les cellules d'adresse respective 83, 84, et 85, l'unité d'information (d,e,f), et l'unité d'information (g,h,i). L'ensemble des deux unités d'information (a,b,c) et (d,e,f) contigües constituent une information I complète telle que par exemple un mot de passe.

Quant à la matrice de dispersion 42, sa taille est fonction du nombre d'unités d'information pouvant être contenues dans la mémoire RAM sécurisée, puisqu'elle comprend, pour chaque unité d'information, une cellule particulière. Dans cet exemple, la mémoire RAM sécurisée comprend quarante-huit cellules, donc trois fois moins d'unités d'information , soit seize cellules B0 à BF. A chaque unité d'information est associée une cellule de la matrice de dispersion qui occupe, dans la zone mémoire considérée, un rang qui est une fonction particulière d'un rang occupé par l'unité d'information dans la mémoire RAM sécurisée 41. Dans cet exemple, la fonction est l'Identité, de sorte qu'à chaque unité d'information est associée une cellule de la matrice de dispersion qui occupe un même rang dans la zone mémoire considérée. Par exemple, à l'unité d'information (a,b,c) qui possède le rang 2 dans la mémoire RAM sécurisée est associée la cellule B1 qui possède le même rang dans la matrice de dispersion. De la même façon, l'unité d'information (d,e,f) est associée à la troisième cellule B2, et l'unité d'information (g,h,i) à la quinzième cellule BE. Mais, dans une variante, ladite fonction G peut être plus complexe, le rang r_j de la cellule de la matrice de dispersion résultant d'une formule mathématique déterminée à partir du rang r_i de l'unité d'information, selon la formule : $r_j = G(r_i)$. Un exemple est le suivant, dans le cas présent où seize rangs sont définis : $r_j = 17 - r_i$

Par définition, l'adresse d'une unité d'information est constituée par l'adresse de la première cellule qu'elle concerne : ainsi, l'adresse de l'unité d'information (a,b,c) de la figure 3 est 83, adresse de sa première cellule contenant l'information (a), tandis que l'adresse de l'unité d'information (g,h,i) est AA. Sur la figure 3, les unités d'information sont disposées à des adresses dites « adresses logiques », correspondant aux adresses qu'il faudra fournir à l'objet portatif pour qu'il traite ces unités d'information. Une procédure d'initialisation de la mémoire RAM 14 va maintenant être exposée, permettant de définir un état initial de rangement des unités d'information dans la mémoire RAM sécurisée 41. Dans une première phase, on remplit la matrice de dispersion 42 avec les adresses des unités d'information pouvant être stockées dans la mémoire RAM sécurisée 41, ces adresses étant tirées de façon aléatoire. Sur la figure 4, seulement trois de ces adresses sont représentées : AA, 92, et 98. Dans une deuxième phase, on rentre les unités d'information à stocker dans la mémoire RAM sécurisée 41, en fonction des adresses contenues dans la matrice de dispersion. Par exemple, on dispose l'unité d'information (a,b,c) à l'adresse contenue dans la cellule de la matrice de dispersion qui est associée à cette unité d'information : nous avons vu qu'il s'agissait de la cellule de rang 2. On dispose donc cette unité d'information à l'adresse AA. De la même façon, on range l'unité d'information (d,e,f) à l'adresse 92, et l'unité d'information (g,h,i) à l'adresse 98. Les adresses contenues dans la matrice de dispersion de la figure 4 sont dites « adresses physiques » car elles vont déterminer l'emplacement réel des unités d'information dans la mémoire RAM sécurisée 41. Sur la figure 4, la mémoire RAM sécurisée 41 est bien dans un état dit « sécurisé » puisque ses unités d'information ont été dispersées par rapport à l'état de la figure 3.

Une autre procédure d'initialisation de la mémoire RAM 14 va maintenant être exposée, en variante. Dans une première phase, on remplit la matrice de dispersion avec les adresses logiques des unités d'information. Ainsi, on met dans la première cellule l'adresse correspondant à la première unité d'information, soit 80. On met dans la deuxième cellule l'adresse

logique correspondant à la deuxième unité d'information (a,b,c), soit 83, etc...Dans une deuxième phase, on remplit la mémoire RAM sécurisée 41 en fonction des adresses contenues dans la matrice de dispersion. Ainsi, et comme représenté sur la figure 3, on range l'unité d'information (a,b,c) au deuxième rang, l'unité d'information (d,e,f) au troisième rang, etc...Enfin, dans une troisième phase, on disperse deux par deux les unités d'information de la mémoire RAM sécurisée 41, en utilisant un procédé de permutation élémentaire décrit plus loin, jusqu'à ce que toutes les unités d'information aient été déplacées. En variante, on aurait pu intervertir les première et deuxième phases.

En fonctionnement, lorsque le microprocesseur exécutera un programme demandant l'accès à une information telle que l'information I précitée en désignant les adresses logiques 83 et 86, le microprocesseur consultera la matrice de dispersion 42. Il lira la première adresse physique écrite dans la cellule de rang 2, à savoir AA, puis il ira lire le contenu de l'unité d'information (a,b,c) à partir de cette adresse en mémoire RAM sécurisée. Puis il lira la seconde adresse physique écrite dans la cellule de rang 3, à savoir 92, puis il ira lire le contenu de l'unité d'information (d,e,f) à partir de cette adresse en mémoire RAM sécurisée : il aura alors reconstitué l'information I.

Selon la première forme de réalisation décrite ci-dessus, on disperse les information dans la mémoire RAM sécurisée en en modifiant la structure, c'est-à-dire l'ordre dans lequel sont disposées les unités d'informations dans les cellules composant l'information considérée, sans toutefois atteindre un degré maximal de dispersion. Au contraire, la variante de la figure 5 permet d'atteindre ce but. Dans cet exemple, chaque unité d'information correspond à une seule cellule de la mémoire RAM sécurisée 41 : il s'ensuit que la matrice de dispersion 44 comprend autant de cellules que la mémoire RAM sécurisée , à savoir quarante-huit, disposées entre les adresses B0 et DF.

Après écriture, dans la matrice de dispersion 44 de l'ensemble des adresses des unités d'information, puis modification aléatoire de ces adresses comme expliqué pour l'exemple précédent, on obtient la matrice de dispersion de la figure 5 où n'ont été représentées que les adresses physiques des neuf unités d'information (a à i) figurant dans la mémoire RAM sécurisée de la figure 3. Par exemple, l'adresse physique de l'unité d'information (b) est stockée dans la cellule de même rang que (b), à savoir le rang 5 : cette adresse est donc 96. De même, l'adresse physique de l'unité d'information (g) est située dans la cellule DA de la matrice de dispersion et vaut 9C.

Ensuite, le microprocesseur de la carte disperse les unités d'information (a à i) dans la mémoire RAM sécurisée, en fonction de l'adresse physique se trouvant dans la matrice de dispersion 44. Par exemple, l'unité d'information (c) est stockée dans la cellule de la mémoire RAM sécurisée 41 dont l'adresse est écrite dans la cellule B5 de la matrice de dispersion 44, à savoir l'adresse 8F. De même, l'unité d'information (f) a pour adresse physique la valeur AB écrite en cellule B8.

On constate que, dans ce deuxième exemple, l'information I formée des six informations élémentaires (a à f) se suivant de façon contigüe sur la figure 3, se trouve décomposée à tel point que les six informations (a à f) ne sont plus du tout contigües. Naturellement, cette propriété est de nature à renforcer la sécurité, puisque le travail d'un fraudeur pour reconstituer le groupe d'informations (a à f) à partir de la mémoire RAM sécurisée , dans l'état où elle se trouve sur la figure 5, est encore plus compliqué qu'à partir de la mémoire RAM sécurisée de la figure 4. En règle générale, plus grand sera le nombre de cellules dans chaque unité d'information, plus faible sera la protection des informations sensibles.

Dans ce qui suit, l'adresse de chaque cellule de chaque zone de la mémoire RAM 14 est définie par un décalage déterminé par rapport à une origine constituée par l'adresse de la première cellule de la zone, ceci en

raison d'un mode d'adressage particulier à un certain type de microprocesseurs. En variante, on pourrait naturellement définir une adresse absolue de chaque cellule, indépendemment des autres cellules, comme cela a été fait en relation avec les figures 3 à 5.

En référence à la figure 6, représentant à nouveau la structure de mémoire RAM de la figure 5, soit pRamSec un pointeur sélectionnant la première cellule 45 de la mémoire RAM sécurisée et pMat un pointeur sélectionnant la première cellule 46 de la matrice de dispersion. Une quelconque cellule de la matrice de dispersion contient une valeur représentant un décalage par rapport au pointeur pRamSec. Supposons que le microprocesseur ait à atteindre le contenu d'une cellule 47 de la mémoire RAM sécurisée dont il connaît l'adresse logique définie comme suit :

pRamSec + décalage logique

L'adresse physique correspondante est donnée par :

pRamSec + décalage physique

sachant que (décalage physique) est égal au contenu de la cellule 48 de la matrice de dispersion qui est homologue de la cellule 47, c'est-à-dire qui possède la même position matricielle ; la cellule 48 a l'adresse suivante : pMat + décalage logique.

On sait désormais déterminer l'adresse physique d'une cellule à adresser, à partir de son adresse logique : une lecture à cette adresse physique nous donne donc une valeur stockée à cette adresse.

On décrit maintenant un procédé préféré pour effectuer une permutation élémentaire du contenu de deux cellules de la mémoire RAM sécurisée tirées au hasard, en regard des figures 7 à 10. Tout d'abord, et comme illustré par l'étape 71 de la figure 7, le microprocesseur 9 effectue un tirage aléatoire de deux nombres parmi un ensemble constitué par les adresses de toutes les cellules de la mémoire RAM sécurisée 41, définies par leur décalage logique : les quarante-huit cellules sont définies par un

décalage logique ayant une valeur comprise entre 0 et 47. Par exemple, les valeurs 4 et 8 sont tirées : elles sont alors stockées dans deux cellules C1 et C2 de la mémoire RAM standard 43, selon l'étape 72 de la figure 7, le résultat étant représenté sur la figure 8. A l'étape 73, le contenu de la cellule de la matrice de dispersion 44 repérée par le décalage logique contenu dans la cellule C1 est stocké dans une cellule C3 de la mémoire RAM standard 43 : le décalage logique étant 4, l'adresse logique correspondante est pMat + 4, relative à la cellule B4 dont le contenu est 22. Le résultat est représenté sur la figure 8. Ensuite, à l'étape 74, on stocke le contenu de la cellule de la matrice de dispersion repérée par la cellule C2 dans la cellule repérée par la cellule C1 : le décalage logique contenu dans la cellule C2 est 8, qui désigne la cellule d'adresse pMat+8, soit la cellule B8 : son contenu 43 est disposé dans la cellule d'adresse pMat+4, soit la cellule B4. Le résultat est représenté sur la figure 9. Enfin, à l'étape 75, le contenu de la cellule C3 est stocké dans la cellule de la matrice de dispersion 44 repérée par le contenu de la cellule C2, à savoir la cellule d'adresse logique pMat+8, soit la cellule B8 : le résultat est représenté sur la figure 10.On peut constater en observant les figures 8 et 10 que les valeurs de décalage logique 22 et 43 ont été interverties.

Une permutation des adresses étant intervenue en matrice de dispersion 44, il faut maintenant effectuer une permutation correspondante des données associées à ces adresses en mémoire RAM sécurisée 41. A l'étape 111 de la figure 11, on lit le contenu de la cellule de la mémoire RAM sécurisée 41 dont l'adresse logique est définie par le contenu de la cellule C1. La valeur de décalage logique 4 renvoie à la cellule B4 de la matrice de dispersion, laquelle contient le décalage physique 43 : l'adresse correspondante en mémoire RAM sécurisée 41 est donc pRamSec + 43, correspondant à la cellule AB. A l'étape 112, le contenu de cette cellule est stocké dans la cellule C3, comme représenté sur la figure 12. A l'étape 113, le microprocesseur lit le contenu de la cellule de la mémoire RAM sécurisée 41 dont l'adresse est définie par le contenu de la cellule C2. La valeur 8

renvoie à la cellule B8 de la matrice de dispersion contenant le décalage physique 22 : l'adresse correspondante en mémoire RAM sécurisée 41 est donc pRamSec + 22, correspondant à la cellule 96, contenant la valeur b. A l'étape 114, cette valeur est stockée dans la cellule de la mémoire RAM sécurisée 41 dont le décalage logique est stocké dans la cellule C1 : le décalage logique 4 correspond an décalage physique 43, lequel désigne la cellule AB de la mémoire RAM sécurisée 41. Le résultat est représenté sur la figure 13. Enfin, à l'étape 115, le microprocesseur stocke le contenu f de la cellule C3 dans la cellule de la mémoire RAM sécurisée 41 ayant le décalage logique stocké dans la cellule C2 : il s'agit de la cellule d'adresse 96. Le résultat apparaît sur la figure 14. En comparant les figures 12 et 14, on peut constater que les valeurs b,f ont bien été permutées.

On peut vérifier sur la figure 14 la correspondance entre les adresses permutées de la matrice de dispersion et les valeurs permutées de la mémoire RAM sécurisée 41. Par exemple, selon la figure 3, la valeur (f) a une adresse définie par le décalage logique 8 soit, sur la figure 14, le décalage physique 22. On peut constater que la valeur f se trouve bien dans la cellule 96 possédant ce décalage physique.

Dans la pratique, le microprocesseur effectuera, non pas une seule, mais un certain nombre de permutations élémentaires constituant une permutation dite « multiple », selon la procédure de la figure 15. A l'étape 151, le microprocesseur tire un nombre aléatoire AL1 : typiquement, ce nombre peut être compris par exemple entre 0 et 256. A l'étape 152, le microprocesseur initialise un compteur avec la valeur AL1. A l'étape 153, le microprocesseur vérifie que le compteur a une valeur positive. Dans l'affirmative, il effectue une permutation élémentaire selon la procédure des figures 7 et 11, en tirant deux nombres aléatoires compris entre 0 et 47. A l'étape 155, le microprocesseur décrémente le compteur d'une unité, puis il retourne à l'étape 153. Une fois que le compteur a atteint la valeur 0, il parvient à la fin de la permutation multiple , repérée en 156.

Le procédé de permutation multiple qui vient d'être décrit, ou procédé de régénération de la matrice de dispersion, sera déclenché à divers moments. Il le sera tout d'abord après chaque remise sous tension de la carte. Il le sera aussi au cours d'une session d'utilisation de la carte, à certains moments critiques, par exemple lorsque l'on traite une information sensible. Ainsi, le chargement du PIN (de l'anglais Personal Identification Number) en mémoire RAM sécurisée 41 suppose le transfert de huit octets vers cette mémoire : on décide de déclencher une régénération de la matrice de dispersion après chargement de chaque octet du PIN. Un autre exemple est celui où une anomalie est détectée dans un registre de sécurité de la carte. On rappelle qu'une carte inclut de façon connue en soi une pluralité de capteurs permettant de tester divers caractéristiques physiques de la carte, par exemple sa température, le taux de rayonnement auquel elle peut se trouver éventuellement soumis, la continuité électrique d'un écran de protection contre les agressions mécaniques, etc...L'état dans lequel se trouvent ces capteurs à un moment donné est enregistré dans ledit registre de sécurité. On peut décider de tester à certains moments critiques l'état du registre de sécurité, par exemple avant de traiter une information sensible et, si une anomalie est détectée, de déclencher une régénération de la matrice de dispersion.

Selon une variante de l'invention, la matrice de dispersion se trouve dans une mémoire de la carte ou du module de sécurité qui est différente de celle constituant la mémoire sécurisée. Ceci est particulièrement avantageux si l'on recherche à économiser la mémoire sécurisée. Par exemple, en référence à la figure 1, la matrice de dispersion pourrait être en mémoire non volatile 10.

On notera qu'un résultat avantageux de l'invention consiste en ce que le temps que met le microprocesseur pour avoir accès à l'une quelconque

des informations stockées dans la mémoire RAM sécurisée 41 est constant. Cela est obtenu en associant les unités d'information à leurs adresses en utilisant une correspondance matricielle (correspondance entre les cellules de la mémoire RAM sécurisée 41 et celles de la matrice de dispersion). Ceci empêche tout fraudeur, observant le microprocesseur, d'effectuer des distinctions entre les accès aux différentes unités d'information, distinctions qui auraient pu lui fournir des renseignements sur les informations manipulées.

REVENDICATIONS

1. Module de sécurité comprenant des moyens de traitement de l'information (9) et des moyens de stockage de l'information (10,14), caractérisé en ce que les moyens de traitement (9) comprennent :

-des moyens pour définir, dans les moyens de stockage (10,14), une première zone mémoire (41) destinée à stocker des informations (a,b,c ; d,e,f), accessibles en désignant des adresses logiques (83,86) ;

-des moyens pour définir, dans les moyens de stockage (10,14), une seconde zone mémoire (42) destinée à stocker des adresses physiques (AA,92) de ces informations définissant leur position dans la première zone mémoire (41), ces adresses physiques étant situées en une position qui est fonction des adresses logiques respectives des informations.

2. Procédé de stockage d'informations dans des moyens de stockage d'information d'un module de sécurité, caractérisé en ce qu'il comprend les étapes consistant à :

-définir, dans les moyens de stockage (10,14), une première zone mémoire (41) destinée à stocker des informations (a,b,c ; d,e,f), accessibles en désignant des adresses logiques (83,86) ;

-définir, dans les moyens de stockage (10,14), une seconde zone mémoire (42) destinée à stocker des adresses physiques (AA,92) de ces informations définissant leur position dans la première zone mémoire (41), ces adresses physiques étant situées en une position qui est fonction des adresses logiques respectives des informations ;

-stocker les informations dans la première zone mémoire (41) en une position qui est fonction de leurs adresses logiques respectives, et les adresses logiques (83,86) de ces informations dans la seconde zone mémoire (42) en une position qui est fonction de ces adresses logiques ; et

-permuter deux à deux les adresses logiques (83,86) des unités d'information (a,b,c ; d,e,f) dans la seconde zone mémoire (42) pour définir leurs adresses physiques et, après chaque permutation, permuter les deux

unités d'information correspondantes dans la première zone mémoire (41), ou vice versa.

3. Procédé de stockage d'informations dans des moyens de stockage d'information d'un module de sécurité, caractérisé en ce qu'il comprend les étapes consistant à :

-définir, dans les moyens de stockage (10,14), une première zone mémoire (41) destinée à stocker des informations (a,b,c ; d,e,f), accessibles en désignant des adresses logiques (83,86) ;

-définir, dans les moyens de stockage (10,14), une seconde zone mémoire (42) destinée à stocker des adresses physiques (AA,92) de ces informations définissant leur position dans la première zone mémoire (41), ces adresses physiques étant situées en une position qui est fonction des adresses logiques respectives des informations ;

-stocker aléatoirement dans la seconde zone mémoire (42) les adresses logiques (83,86) des informations pour définir des adresses physiques de ces informations ; et

-stocker les informations dans la première zone mémoire (41) en une position qui est fonction de leurs adresses physiques respectives.

4. Procédé d'exploitation d'informations dans des moyens de stockage d'information d'un module de sécurité, dans lequel on a défini, dans les moyens de stockage (10,14), une première zone mémoire (41) destinée à stocker des informations (a,b,c ; d,e,f), accessibles en désignant des adresses logiques (83,86) et on a défini, dans les moyens de stockage (10,14), une seconde zone mémoire (42) destinée à stocker des adresses physiques (83,86) de ces informations définissant leur position dans la première zone mémoire (41), ces adresses physiques étant situées en une position qui est fonction des adresses logiques respectives des informations, caractérisé en ce qu'il comprend l'étape consistant à accéder à toute

information (a,b,c ; d,e,f) désignée par son adresse logique (83,86) en lisant son adresse physique (AA,92) dans la seconde zone mémoire (42).

5. Procédé d'exploitation selon la revendication 4, comprenant l'étape consistant à modifier périodiquement et de façon aléatoire la position des adresses physiques (AA, 92) des unités d'information (a,b,c ; d,e,f) dans la seconde zone mémoire (42), et à modifier de façon correspondante la position des unités d'information dans la première zone mémoire (41).

6. Procédé d'exploitation selon la revendication 5, dans lequel la modification périodique de la position des adresses physiques (AA,92) et des unités d'information (a,b,c ; d,e,f) est déclenchée lors du traitement d'une information sensible.

7. Procédé d'exploitation selon la revendication 5, consistant à permuter deux à deux les adresses physiques (AA, 92) des unités d'information (a,b,c ; d,e,f) dans la seconde zone mémoire (42) et, après chaque permutation, permuter les deux unités d'information correspondantes dans la première zone mémoire (41).

8. Procédé d'exploitation selon la revendication 4, dans lequel on stocke dans la première zone mémoire (41) des unités d'information (a,b,c) ayant une taille inférieure à une taille des informations (a,b,c,d,e,f), lesdites unités d'information étant accessibles en désignant lesdites adresses logiques (83,86) et étant stockées dans une position définie par lesdites adresses physiques (AA,92).

9. Procédé d'exploitation selon la revendication 8, dans lequel lesdits moyens de stockage comprennent plusieurs cellules (45,47) et chaque unité d'information a une taille telle qu'elle est stockée dans une seule

cellule (47) de la première zone mémoire (41) et son adresse physique est stockée dans une seule cellule (48) de la seconde zone mémoire (42).

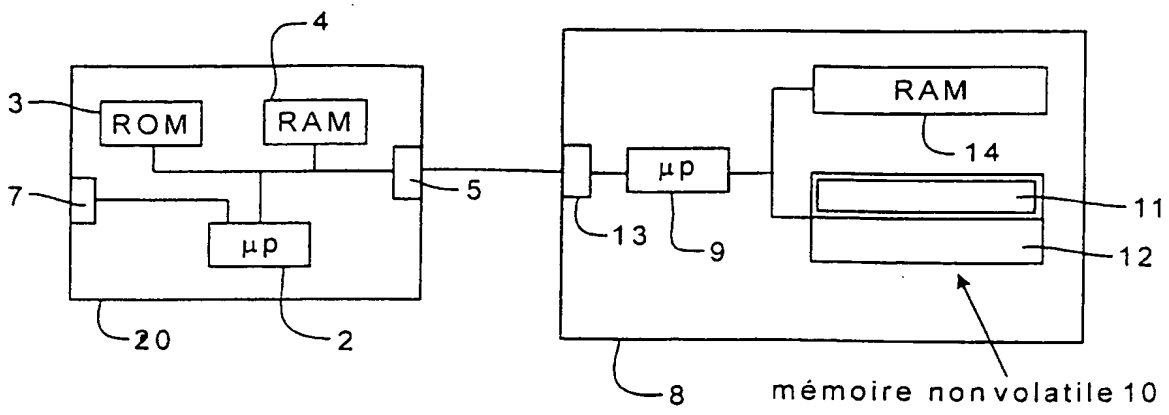

4
3
ROM
RAM
7
5
µp
20
2
RAM
14
µp
11
13
9
12
8
mémoire non volatile 10

Fig.1

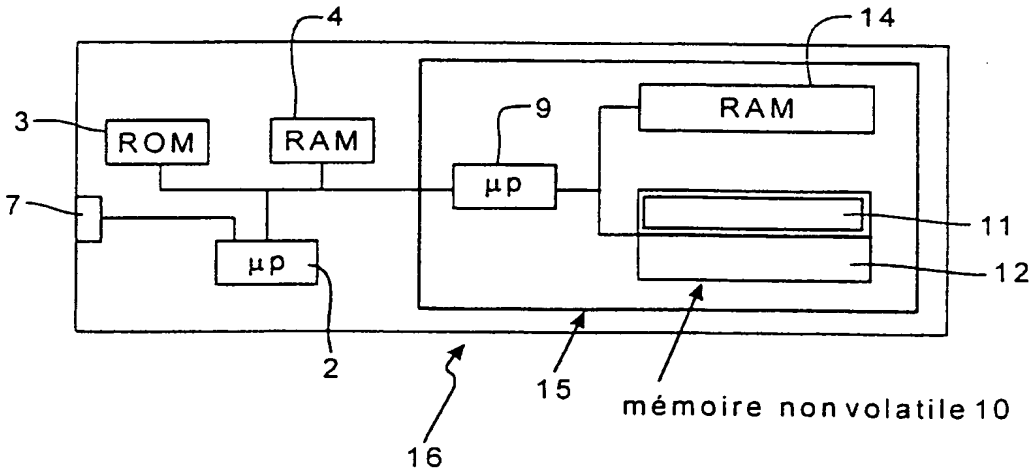

4
14
3
ROM
RAM
9
RAM
µp
7
11
µp
12
2
15
mémoire non volatile 10
16

Fig.2

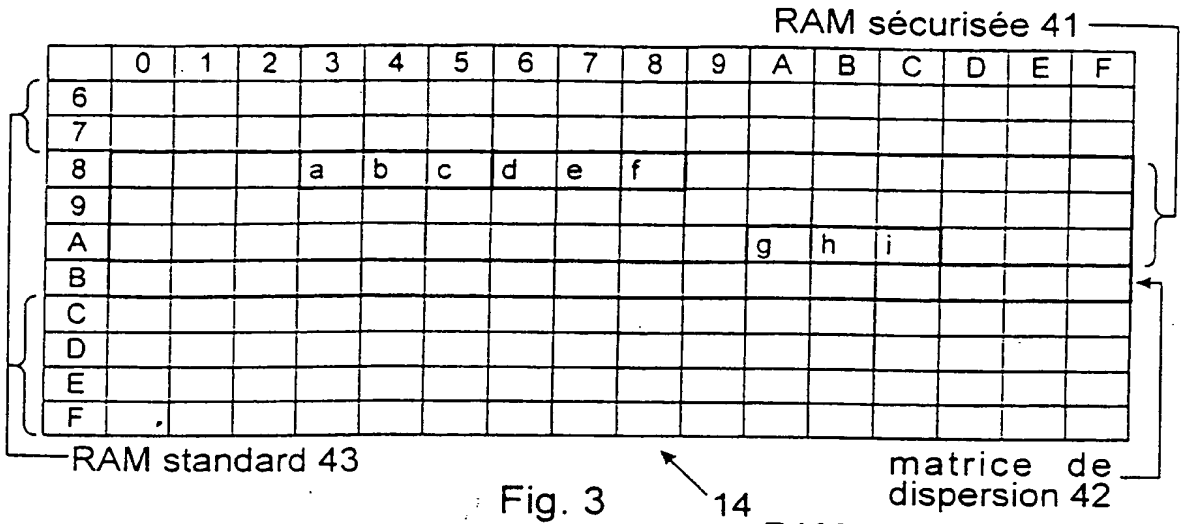


Fig. 3

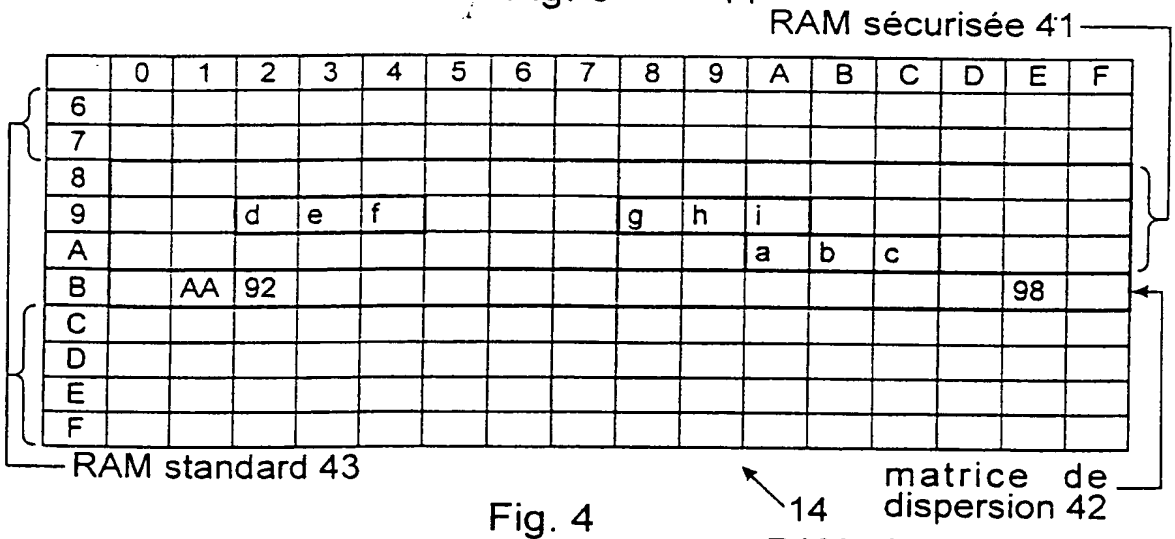


Fig. 4

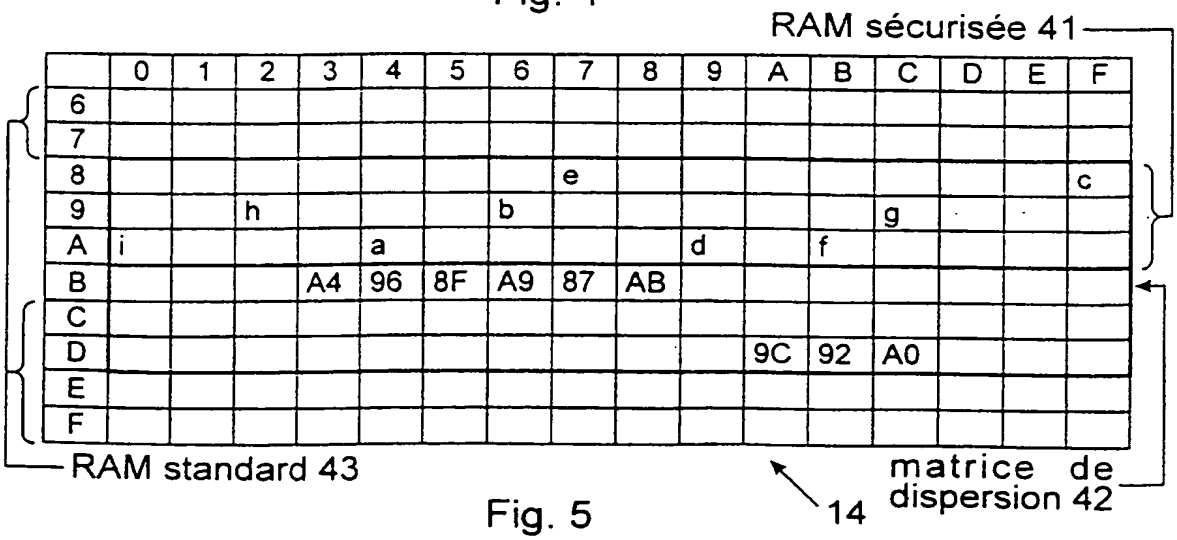


Fig. 5

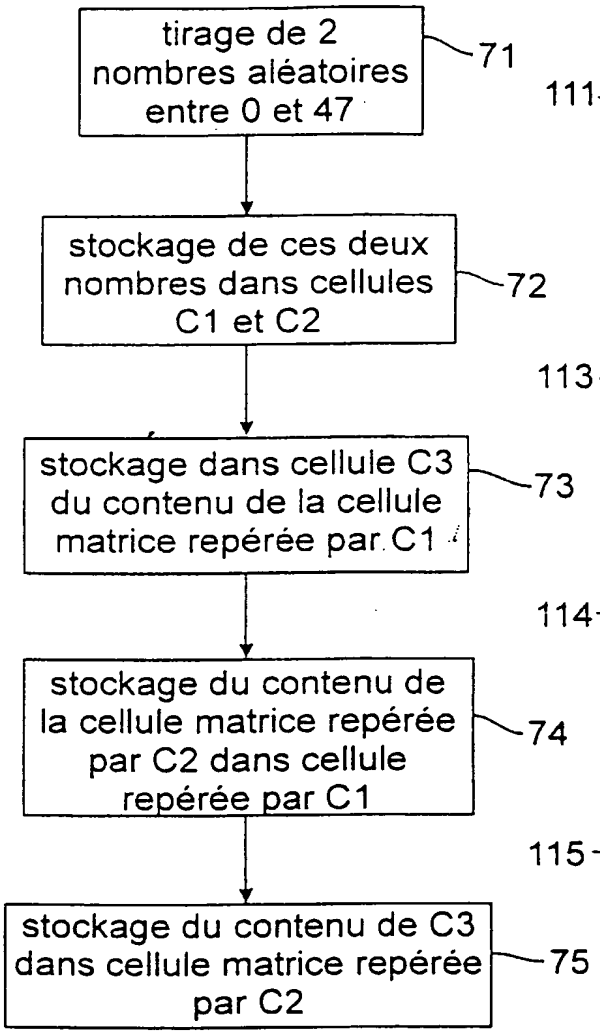


Fig. 7

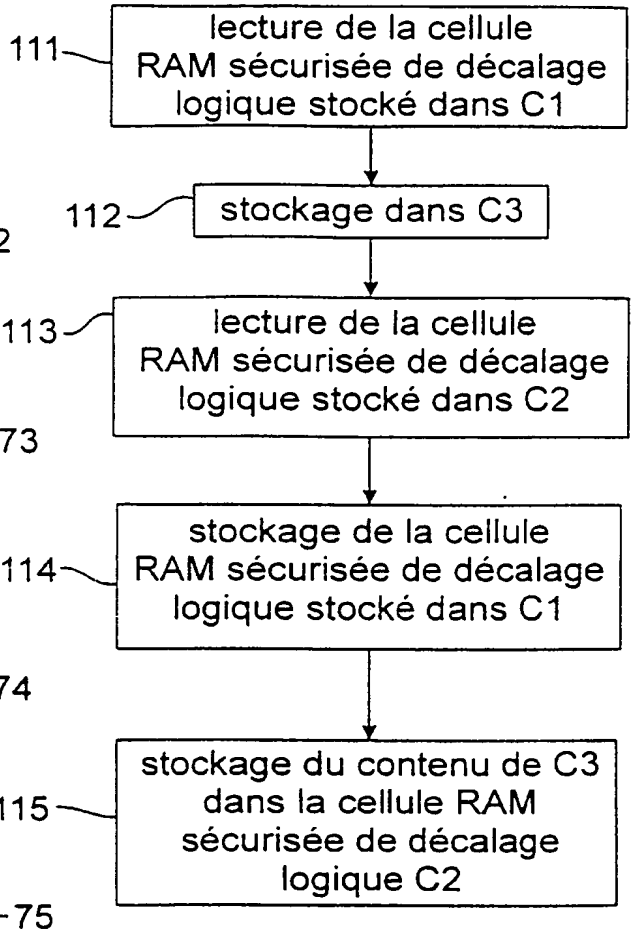


Fig. 11

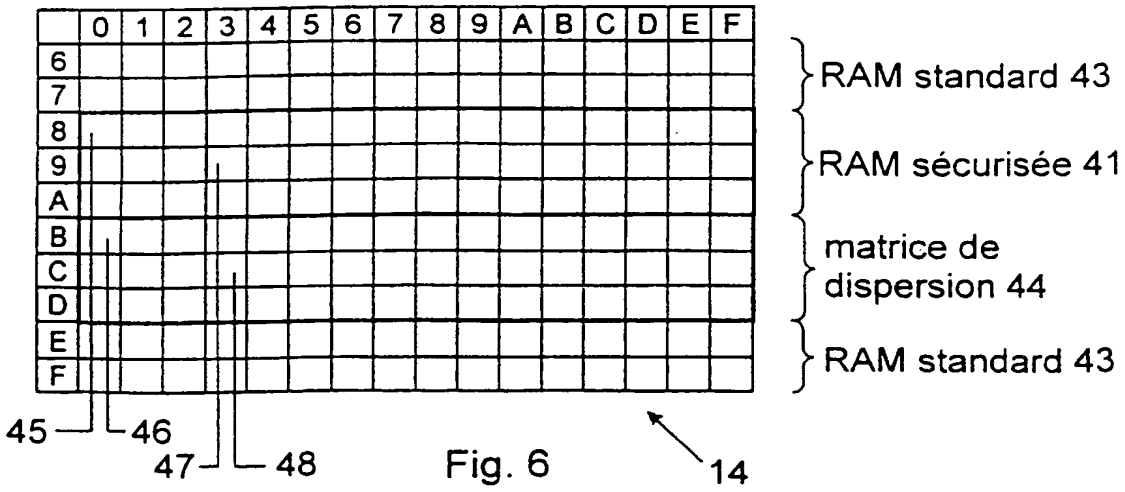
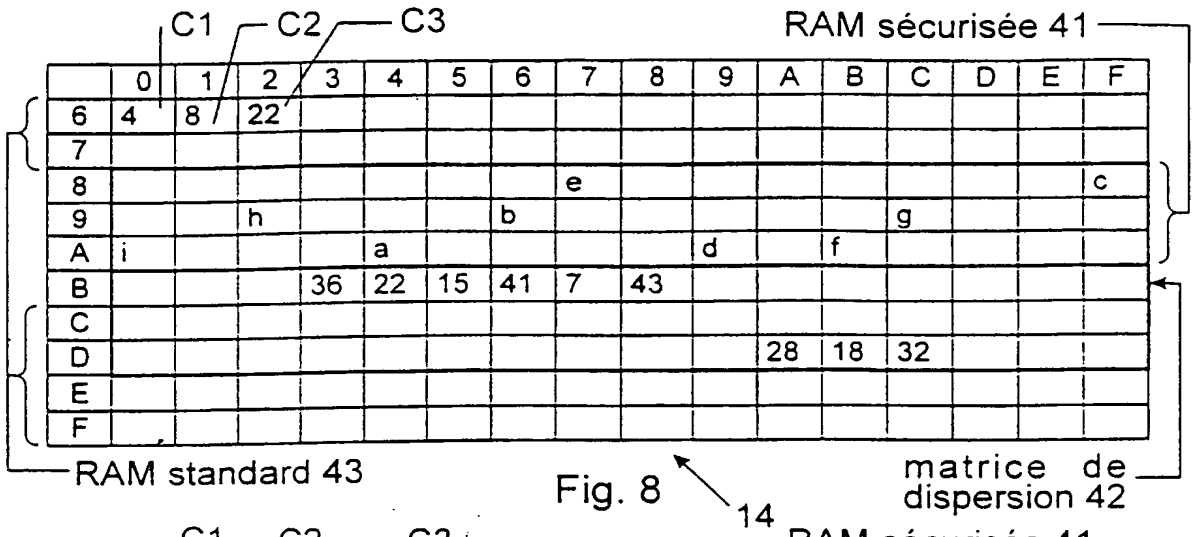
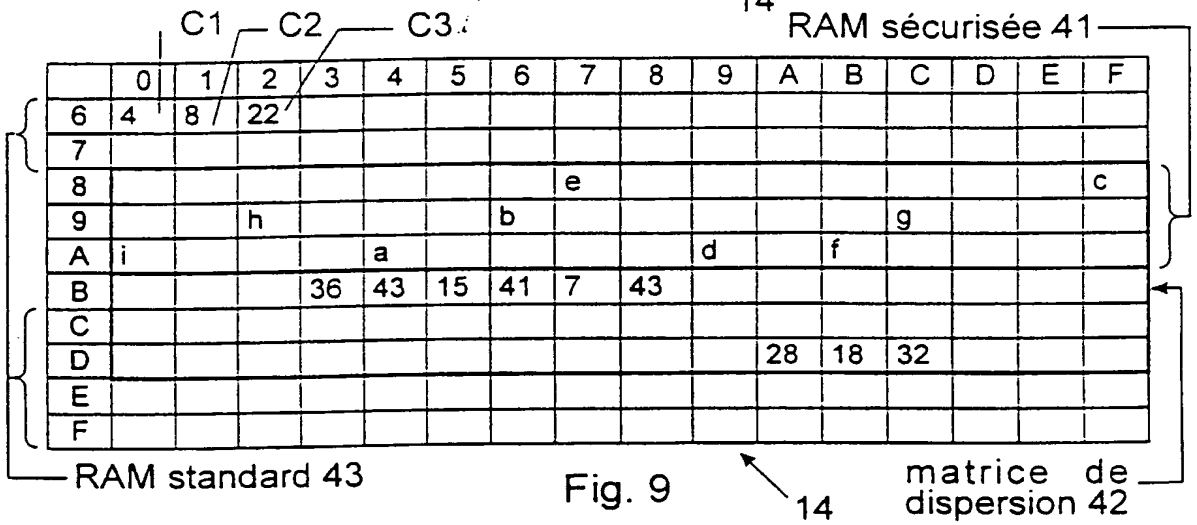


Fig. 6



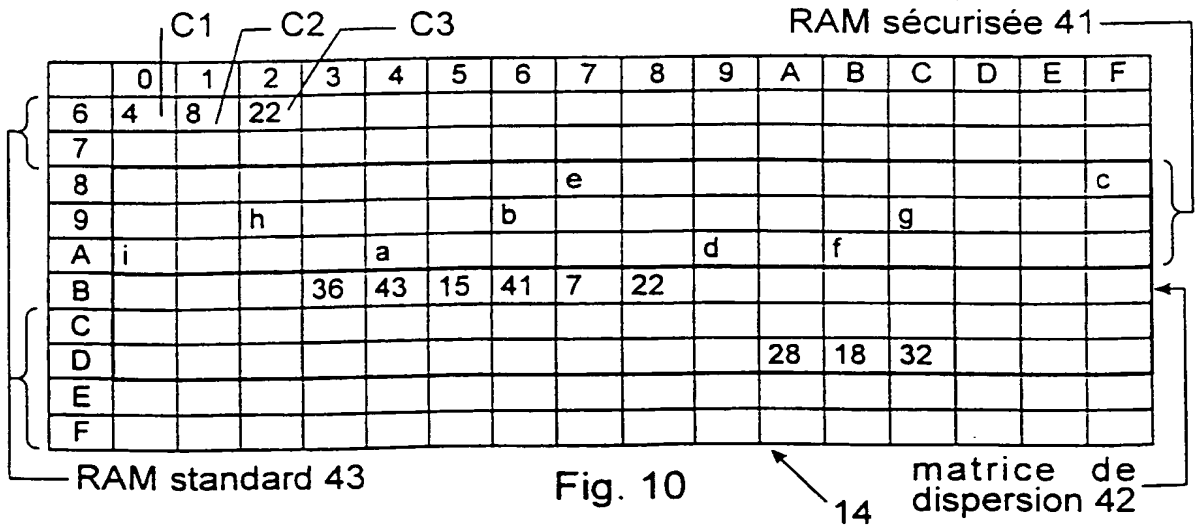
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
6	4	8	22													
7																
8								e								c
9			h				b						g			
A	i				a					d		f				
B				36	22	15	41	7	43							
C																
D											28	18	32			
E																
F																

Fig. 8



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
6	4	8	22													
7																
8								e								c
9			h				b						g			
A	i				a					d		f				
B				36	43	15	41	7	43							
C																
D											28	18	32			
E																
F																

Fig. 9



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
6	4	8	22													
7																
8								e								c
9			h				b						g			
A	i				a					d		f				
B				36	43	15	41	7	22							
C																
D											28	18	32			
E																
F																

Fig. 10

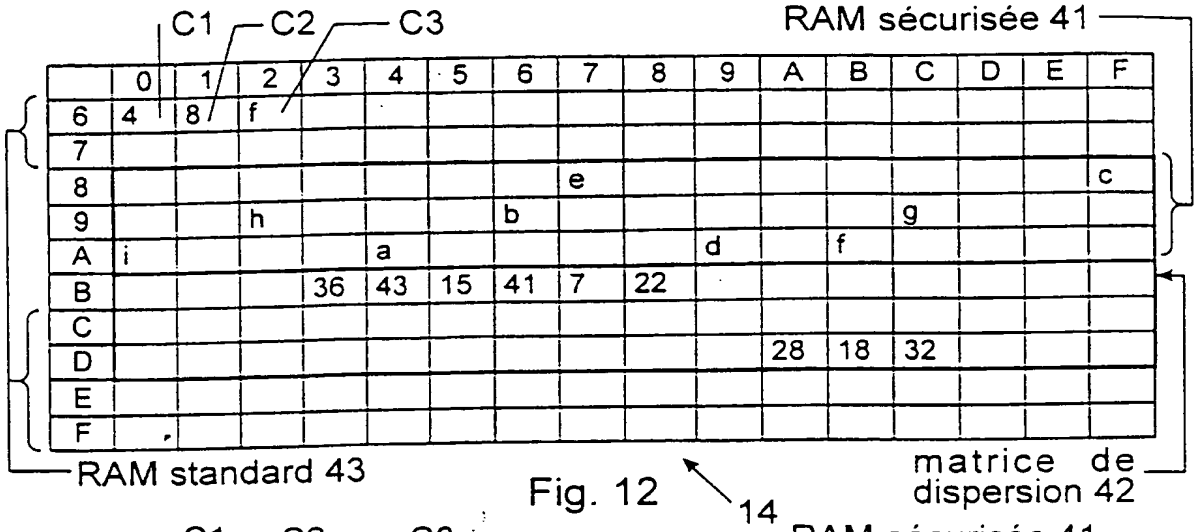


Fig. 12

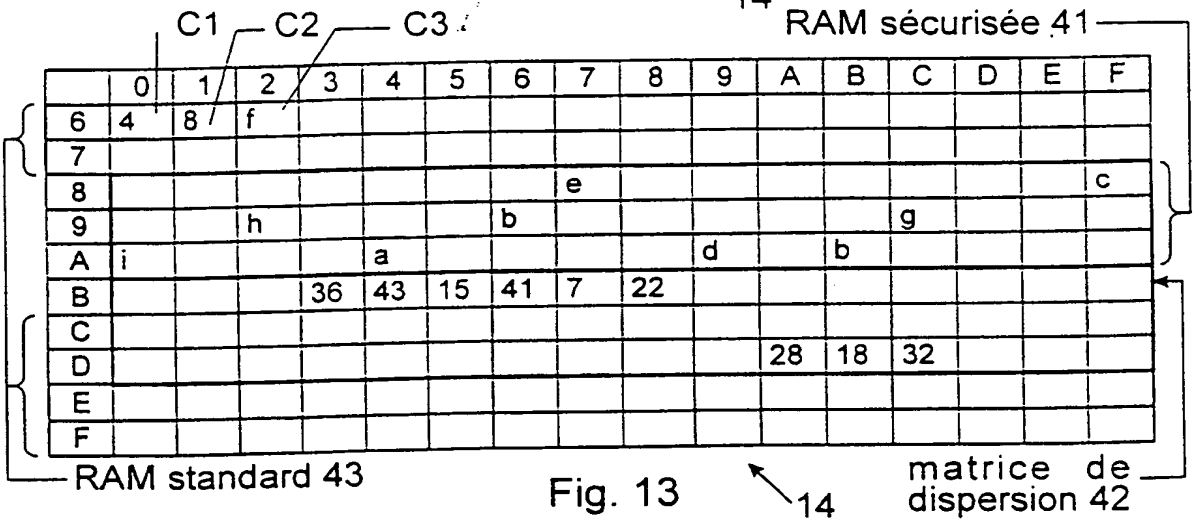


Fig. 13

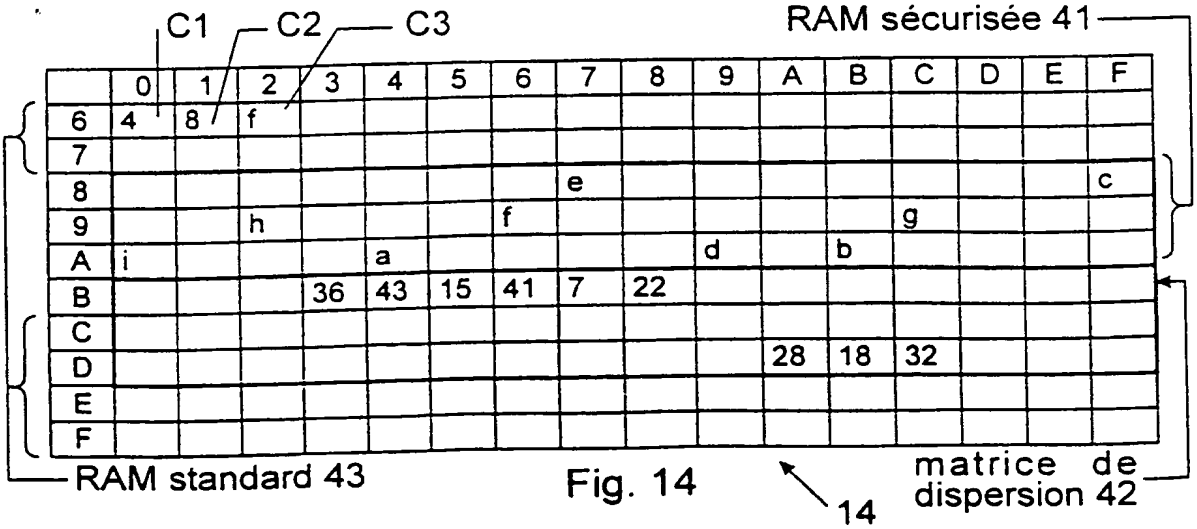


Fig. 14

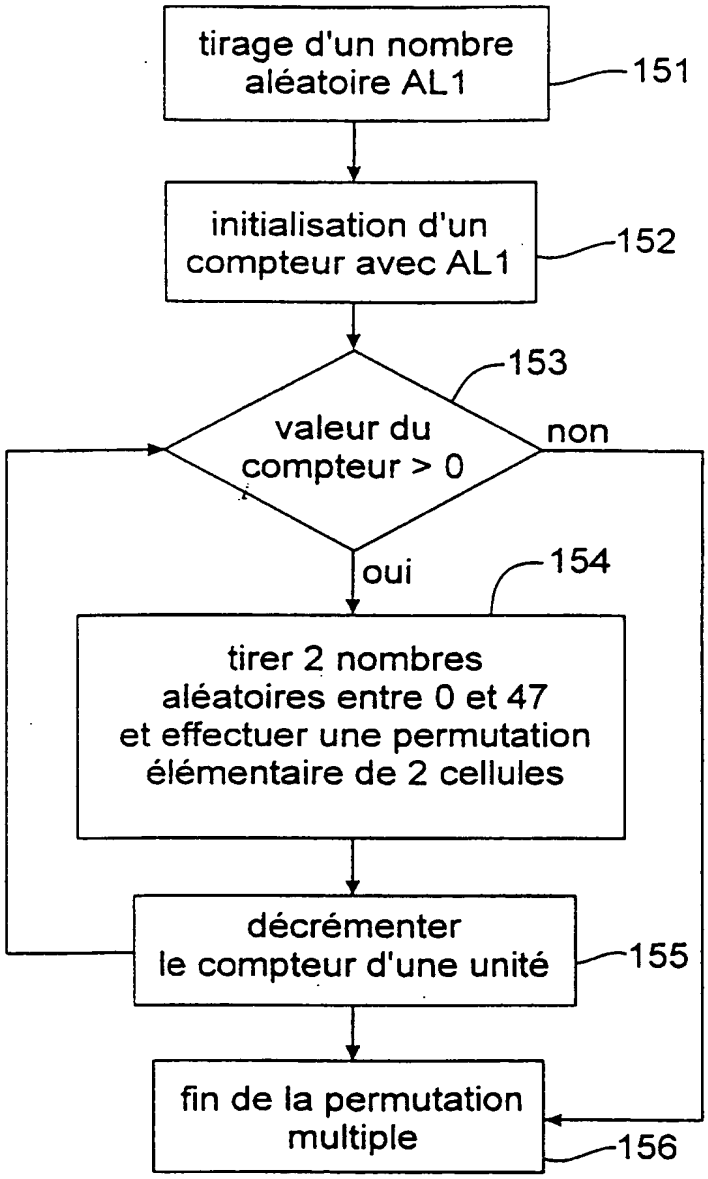

tirage d'un nombre aléatoire AL1
151
initialisation d'un compteur avec AL1
152
153
valeur du compteur > 0
non
oui
154
tirer 2 nombres aléatoires entre 0 et 47 et effectuer une permutation élémentaire de 2 cellules
décrémenter le compteur d'une unité
155
fin de la permutation multiple
156

Fig. 15

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/FR 99/03086

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F11/20 G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 064 558 A (HUGHES WILLIAM C ET AL) 20 December 1977 (1977-12-20) abstract; figure 2 column 1, paragraph 3 -column 3, paragraph 1 ---	1,3-5,8, 9
A	WO 93 23806 A (IBM) 25 November 1993 (1993-11-25) abstract; figures 1-3 claims 1-22 ---	1-5,7,8
A	US 5 081 675 A (KITTIRUTSUNETORN KITTI) 14 January 1992 (1992-01-14) abstract; figures 2-8 column 11, line 54 -column 12, line 45 claims 1-20 --- -/--	1,4,8,9

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 March 2000	15/03/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/FR 99/03086

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 568 438 A (GEMPLUS CARD INT) 3 November 1993 (1993-11-03) the whole document	1-9

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/FR 99/03086

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4064558 A	20-12-1977	NONE	
WO 9323806 A	25-11-1993	EP 0640228 A	01-03-1995
		JP 7503564 T	13-04-1995
US 5081675 A	14-01-1992	NONE	
EP 0568438 A	03-11-1993	FR 2690540 A	29-10-1993
		DE 69326497 D	28-10-1999
		DE 69326497 T	10-02-2000

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 99/03086

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F11/20 G06F12/14

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 4 064 558 A (HUGHES WILLIAM C ET AL) 20 décembre 1977 (1977-12-20) abrégé; figure 2 colonne 1, alinéa 3 -colonne 3, alinéa 1	1,3-5,8, 9
A	WO 93 23806 A (IBM) 25 novembre 1993 (1993-11-25) abrégé; figures 1-3 revendications 1-22	1-5,7,8
A	US 5 081 675 A (KITTIRUTSUNETORN KITTI) 14 janvier 1992 (1992-01-14) abrégé; figures 2-8 colonne 11, ligne 54 -colonne 12, ligne 45 revendications 1-20	1,4,8,9

-/---

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
7 mars 2000	15/03/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Powell, D

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Dem: Internationale No
PCT/FR 99/03086

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 568 438 A (GEMPLUS CARD INT) 3 novembre 1993 (1993-11-03) le document en entier	1-9

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dem. internationale No
PCT/FR 99/03086

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 4064558 A	20-12-1977	AUCUN	
WO 9323806 A	25-11-1993	EP 0640228 A	01-03-1995
		JP 7503564 T	13-04-1995
US 5081675 A	14-01-1992	AUCUN	
EP 0568438 A	03-11-1993	FR 2690540 A	29-10-1993
		DE 69326497 D	28-10-1999
		DE 69326497 T	10-02-2000